Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

gemalto
security to be free

Protection of unstructured data

Associated challenges and solutions by Capgemini and Gemalto

People matter, results count.

Protect your data

With the General Data Protection Regulation (GDPR) looming ahead, organizations are reeling under both existing and perceived pressures. Capgemini and Gemalto jointly bring to you a whitepaper aimed at explaining the possible implications of the legislation and how it impacts the way your organization protects its data. Capgemini and Gemalto will present a combined set of products, services, and technological offerings that can help you prepare for the GDPR and protect your data – unstructured data, in particular. First, we will explain why the GDPR is important to your organization. Second, we will discuss how unstructured data can be protected and its associated challenges. Third, we will illustrate several organization scenarios and discuss their preparations for the GDPR. Fourth, we will explain our portfolio and demonstrate how this can help your organization get ready for the GDPR.

Why the GDPR is important for your organization

The GDPR, an EU wide framework for the protection and free movement of personal data of EU citizens, will be enforced from May 2018. It requires a very systematic and comprehensive management of data security, including data protection management, reporting, and accountability mechanisms, as also a requirement to notify data breaches, map data flows, and conduct data protection impact assessments. Many organizations will be required to recruit a Data Protection Officer (DPO). More importantly, a data subject’s consent to the use of his or her personal data should be given via a clear affirmative act. The GDPR provides enhanced rights for individuals and increased scrutiny by regulators. Failing to comply with the GDPR can lead to fines of up to 4 percent of the worldwide turnover or 20 million euro, whichever is higher.

Why is it important to protect unstructured data?

Organizations hold various types of data, for example structured data in databases and unstructured data in files, (shared) folders, emails, and desktops, etc. It is estimated that unstructured information might account for more than 70%-80% of all data in organizations. In recent years, security breaches have become increasingly common and more severe.

Legislations such as the GDPR require that security measures to protect personal data should correspond to an appropriate level of risk and the damage a breach would cause to an individual.

Traditional network security measures, such as network firewalls and other perimeter protection are insufficient in protecting personal data. Data encryption is therefore also becoming increasingly important. Encryption is a proven method of protecting data by attaching security to the data itself, whereby the data remains completely secure wherever it travels. Encrypting will ensure that the data is unusable except when possessing the encryption key. For unstructured data, several encryption options are available, with file and application encryption being the most commonly applied.

Some practical examples

Gemalto and Capgemini work with organizations from all industries across the globe. Together, we have a deep understanding of the GDPR, and the challenges associated with the protection of unstructured data. Below are three hypothetical examples where we illustrate how Gemalto's and Capgemini's combined offerings can assist you in protecting your unstructured data and preparing for the GDPR. The challenges described in these organizations reflect the preparatory work we see in practice.

Example 1 - Multinational insurance company

A multinational insurance company required a solution for personal data of its customers. It has a large application landscape with data stored in databases and in files, folders, and shared drives. The company holds personal data of policyholders and it knows the location and nature of this data. The company has recently experienced a data breach where a vulnerability was exploited to access files, which, luckily, did not contain any personal data. To protect against future breaches, the company wanted a solution that was able to encrypt unstructured data files, such as word processing documents, spreadsheets, images, and more. It wanted to ensure that only authorized users could access this sensitive information. The company asked Capgemini to support the implementation of a file encryption solution to encrypt its sensitive data in combination with centralized key and policy management. For this purpose, Capgemini partnered with Gemalto. As a result, teams working on highly sensitive projects can collaborate productively with the confidence that their files remain secure. When employees record customer data in a document, it is first encrypted and stored. The file can only be accessed by authorized users or applications based on policies set by administrators.

Example 2 - Multinational utilities company

A leading global utilities company wanted to deploy a data protection solution that included both encryption and key management to protect customer data stored in the cloud. It wanted to not only protect its customer data but also maintain full ownership of the data in order to meet requirements following from the GDPR. The company additionally wanted flexibility in its systems, so as to add any future cloud service providers and additional users as and when required. Capgemini was asked to support with the implementation of a strong encryption and key management solution for data in the cloud. Capgemini worked with Gemalto to implement key management technology and virtual machine encryption. The key management solution was independent from the cloud provider in order to maintain full ownership and control of the data and encryption keys at all times. Finally, Capgemini implemented a solution to encrypt the entire virtual machine instance, including attached storage volumes, as well as the required authorization of a user before launching a virtual machine. As a result, the company is reaping the benefits of cloud computing whilst keeping its most sensitive data secure.

Example 3 - National health care company

A national health care company within the EU holds a significant amount of personal data of its clients, including medical records and other highly sensitive data. The company started preparations for the GDPR and identified gaps in terms of the people, process, technology, data and governance when it conducted a GDPR readiness assessment. The company requested Capgemini to facilitate the development of a roadmap to implement solutions to meet the GDPR requirements. Capgemini organized a one day workshop bringing together key stakeholders from the company to develop the overall roadmap.
As a result work packages per stream were outlined, and governance and stakeholders were determined. An overall plan was created with the above mentioned streams, work packages, and milestones. Using this approach allowed the company to get the roadmap for GDPR readiness in place with full buy-in from the crucial stakeholders.

How can we support?

Gemalto and Capgemini are partnering to help you get ready for the GDPR and protect your data. We have designed a combined set of offerings to help prepare for the new regulation, irrespective of whether you are ready for the change or still have a long way to go. Our portfolio considers the most important topics regarding the protection of data, and consists of four main categories:

- Discovery
- Remediation
- Data subject rights
- Readiness

Discovery

GDPR Assessment

Capgemini proposes an assessment which provides an analysis and recommendations on planning, governance, process, culture, data, and technology. The assessment is performed by a team of three specialists and can be finalized in a four-week period. The team will collect and analyze the available materials on the aforementioned categories, perform data discovery to find where personal data is located in the organization, and interview key persons responsible for these areas in the light of the GDPR. The assessment will provide insight into the level of GDPR readiness and which personal data the organization is holding. The result of the assessment is a list of categorized findings and actionable recommendations to prepare for the GDPR. In particular, the following areas will be assessed:

- Individual Rights: review and assess your internal processes to determine whether they meet the requirements of individuals' rights (e.g., providing consent, how to grant access to data).
- Data Breach Notification requirements: review and assess your organization's readiness with respect to the new GDPR rules regarding data breach notification to Supervisory Authorities and individuals.
- Record Keeping: review and assess your organization's current databases, records, and archives to see what is in place and what is missing to meet the new records requirements.
- Data Protection Officer ("DPO"): assess the need for your organization to have a DPO and review the current position of a DPO (if any) to evaluate what organizational changes may be required.
- Consent and Notice: review customer-facing materials to comply with new consent and transparency requirements (and if applicable, particularly with respect to data analytics, profiling, free services, and digital offerings to children).
- Third Party Agreements: review and update agreements and templates with your organization's data processors (suppliers, partners, etc.).

GDPR road map

Capgemini proposes to include a set of defined action items that employ the use of technology to raise the quality and level of personal data protection within your organization into your strategic plan for the GDPR. The development of the plan will involve the stakeholders of your organization and result in a realistic, supported, and actionable plan. Capgemini will facilitate plan development and use its experience of strategic plan development, GDPR readiness capabilities, and experienced insight into your business and technology solutions. A data security road map can be developed in two to four weeks – or in a two-day concentrated workshop with all stakeholders.

Remediation

Capgemini proposes the project management, and Gemalto the technical implementation of its solution for the protection of unstructured data in files, applications, and virtual machines by means of encryption. The combined offering provides the following benefits:

- Application-level encryption: the solution encrypts data at the application level to secure personal data as it is created. It provides standard encryption and key management interfaces to protect both structured and unstructured data in any environment.
- File encryption: the solution provides transparent, automated file system-level encryption with policy based access controls for files, folders, or network shares on file servers, virtual machines, and in big data technologies.
- Centralized enterprise key management: the solution is an encryption and key manager, available either as hardware or as a virtual appliance, which streamlines encryption management across the enterprise. It helps eliminate silos within an organization and puts administrators in full control of the data to ensure that it is used only as authorized and is protected from a variety of threats.
- Virtual machine encryption: As files reside on a virtual machine, it is possible to secure the entire virtual machine instance for everything contained within. This is similar to full disk encryption, except that here it is applicable for a virtual machine. This ensures that a virtual instance cannot be copied and replicated in an unauthorized environment to expose the sensitive (personal) data. It is an effective form of security for virtual machines used primarily for backup and storage.

Data subject rights

Right to be forgotten and data erasure

Capgemini's process-solutions meet the requirements in the GDPR related to data subject rights, particularly the right to be forgotten and the right to erasure. We will define and automate the process flow for identification, alerting, reporting, and escalation of an individual's request for the right to be forgotten and data portability. Tasks are assigned to system administrators and the data protection officer, and a dashboard is delivered to provide end-to-end process monitoring. The solution will allow demonstrable compliance and support audit or review.

Consent management

Capgemini proposes to deploy a platform for consent management to allow customers to manage, approve, review, or withdraw consent. Capgemini will implement the consent management platform and integrate this with the service portals of the organization. This provides a central place to give consent for attribute sharing, for consent overview and reporting, and for preference management.

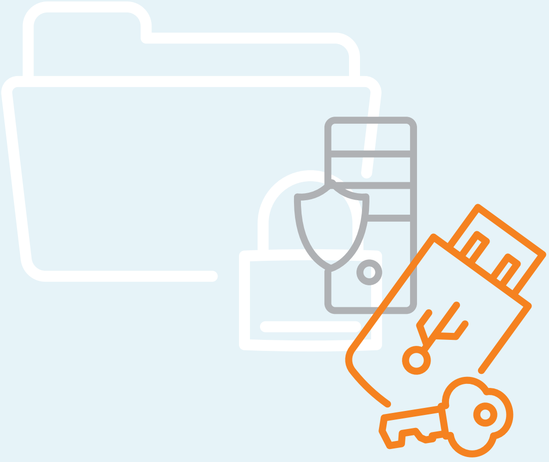
Readiness

Breach management

Capgemini proposes to implement a data breach management model which includes: incident recording, authority notification, and securing documentation and artifacts in case of breach. Key staff members will be trained by means of exercises and simulations, to be able to adequately respond in case of a data breach. This way your organization will be trained for better incident response, crisis, and business continuity management.

Privacy & security awareness

Capgemini proposes to conduct a privacy and security awareness program to enhance awareness of privacy and cyber security across the enterprise to further increase GDPR readiness and better protection of data subjects. That will include a tailor-made classroom training, online training, and specialized training for persons with a specific responsibility in the context of the GDPR or security. The program will focus on the key staff members such as the data protection officers (DPO), database administrator (DBA), and (senior) management, as a result of which these key staff members will be better aware of their responsibilities following the implementation of GDPR.



Please contact us for more information:

Kim Boermans
Capgemini Nederland B.V.
kim.boermans@capgemini.com

Christian Kuhn
Gemalto
christian.kuhn@gemalto.com

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

About Capgemini

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR 12.5 billion.

Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

About Gemalto

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2016 annual revenues of €3.1 billion and customers in over 180 countries. We bring trust to an increasingly connected world. From secure software to biometrics and encryption, our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between. Gemalto's solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things. Our 15,000+ employees operate out of 112 offices, 43 personalization and data centers, and 30 research and software development centers located in 48 countries.

Learn more about us at
www.nl.capgemini.com

For more details contact:

Capgemini Nederland B.V.
P.O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.nl.capgemini.com

People matter, results count.